## AMENDMENT TO CLAIMS

1. (Currently Amended) A method, comprising:

determining security information associated with at least one object of a transaction, wherein the object is to be transmitted from a source device to a target device along a transmission path that includes at least one intermediate device;

determining if an adjacent intermediate ~~a remote~~ device in the transmission path is capable of providing a level of security indicated by at least a portion of the security information; and

transmitting the object to the adjacent intermediate ~~remote~~ device in the transmission path in response to determining that the adjacent intermediate ~~remote~~ device is capable of providing the level of security.

2. (Currently Amended) The method of claim 1, wherein the object is a business object, and wherein determining if the adjacent intermediate ~~remote~~ device in the transmission path is capable of providing the level of security comprises:

transmitting to the adjacent intermediate ~~remote~~ device in the transmission path information representative of the level of security that is desired; and

receiving a response from the adjacent intermediate ~~remote~~ device in the transmission path indicating that the adjacent intermediate ~~remote~~ device in the transmission path is capable of providing the desired level of security.

3. (Currently Amended) The method of claim 1, wherein determining the security information comprises accessing a header portion of the object;

wherein determining if an adjacent intermediate device in the transmission path is capable of providing a level of security indicated comprises performing at least one of:

transmitting information representative of the level of security that is desired to the adjacent intermediate device in the transmission path prompts the adjacent intermediate device in the transmission path to execute at least one module that allows the adjacent intermediate device in the transmission path to provide the level of security; and

comparing the adjacent intermediate device in the transmission path to a list of trusted devices in the header portion of the object;

wherein transmitting the object to the adjacent intermediate device in the transmission path comprises transmitting the object to an object handler module in the adjacent intermediate device in the transmission path;

wherein the object handler module is a business integration adapter supporting connectivity options, the connectivity options comprising at least one of packaged applications, custom applications, legacy applications, databases, trading partners' systems, and public information stores on the internet;

wherein the object handler module supports at least one of event-driven real-time synchronous connections, asynchronous loosely coupled connections with trading partners, synchronous on-demand connections to customers and synchronous tightly coupled connections to trusted trading partners;

wherein the object handler module includes at least one of a module for accessing the security information associated with a given object and a module for requesting the adjacent intermediate device in the transmission path to provide information about its security capabilities.

4. (Original) The method of claim 3, wherein determining the security information comprises determining security information relating to at least one of connection information, class information, trusted entities information, and logging capability information.

5. (Original) The method of claim 3, wherein accessing the header portion of the object comprises accessing at least one header of a Simple Object Access Protocol message.

6. (Currently Amended) The method of claim 1, further comprising determining an alternative intermediate ~~remote~~ device along a different transmission path that is capable of providing the level of security represented in response to determining that the adjacent intermediate ~~remote~~ device in the transmission path is not capable of providing the level of security.

7. (Currently Amended) The method of claim 1, further comprising sending a message to the adjacent intermediate device in the transmission path ~~causing~~ instructing the adjacent intermediate ~~remote~~ device to execute at least one module that allows the adjacent intermediate ~~remote~~ device to provide the level of security.

8. (Currently Amended) The method of claim 1, wherein determining the security information comprises determining the security information in response to receiving the object from at least one of a previous remote device and a source.

9. - 27. (Cancelled)

28. (Currently Amended) A method, comprising:

receiving, at a first device, a request from a second device desiring to transmit at least one object to a third device, wherein the request includes at least a portion of security information associated with the object;

determining if the first device is capable of providing a level of security represented by the security parameter; and

transmitting an indication to the second device based on determining if the first device is capable of providing the level of security.

29. (Original) The method of claim 28, further comprising configuring the first device with at least one module that allows the first device the capability of providing the level of security.

30. (Original) The method of claim 29, further comprising receiving the data object from the second device.